MISSION 6 : DÉCOUVERTE ET ANALYSE DE RÉSEAU

Cette mission fait l'objet d'un compte rendu au format PDF (AP1-Mission-6-*NOM-Prénom*.pdf) qui fera apparaître, selon le cas, une réponse à la question ou une capture d'écran de la commande et son résultat.

Objectif

L'objectif de cette mission est de découvrir et d 'analyser le réseau de la société XILIM.

Partie 1 : Vérification de quelques connaissances de base

1. Rendez-vous sur bit.ly/1btsAP1M6bis pour vérifier vos connaissances de base avant de continuer. (Respecter les caractères majuscules ou minuscules en recopiant le lien).

Partie 2 : Collecter des informations sur votre machine au sein d'un réseau

La commande ip est un outil réseau Linux destiné aux administrateurs système et réseau. IP signifie Internet Protocol et, comme son nom l'indique, cet outil est utilisé pour configurer les interfaces réseau. Les anciennes distributions Linux utilisaient la commande ifconfig, qui fonctionne de manière similaire. Cependant, ifconfig a une gamme limitée de capacités par rapport à la commande ip.

Démarrer votre machine virtuelle sur Linux

2. Utilisez la commande ip help pour voir la liste des options de la commande ip disponibles. Notez celle qui vous semble la plus utile.
3. Déduisez la commande utilisée pour afficher votre adresse ip. Exécutez-là et notez votre adresse IP.
4. Déduisez la commande utilisée pour afficher votre passerelle par défaut. Exécutez-là et notez votre passerelle par défaut.
5. Utiliser la commande ip link help pour voir les options disponibles concernant les interfaces réseau
6. Déduisez la commande utilisée pour montrer l'état de toutes les interfaces réseau du système.
7. Avez-vous remarqué que cette dernière commande vous donne l'adresse MAC de votre machine ? Non ? Exécuter à nouveau et notez-là.
8. Déduisez la commande utilisée pour voir uniquement la liste des interfaces en cours d'exécution. Exécutez-là et notez vos interfaces disponibles.
9. Que fait la commande ip link set [interface] up ?
10. Donnez la commande pour désactiver une interface (hors ligne).

11. A partir de la commande ip help, trouvez et exécutez la commande pour afficher la table de routage.
12. La commande ci-après ip a show > /home/euphraim/Bureau/ip.txt permet d'enregistrer l'adresse ip dans un fichier sur le Bureau d'une VM Linux. Adapter la commande pour enregistrer l'adresse MAC des interfaces actives dans le fichier mon-address-mac sur votre Bureau.
13. Sur la base de l'annexe de l'AP, trouvez le constructeur de l'adresse MAC de votre carte réseau. Notez le nom du constructeur.

Partie 3 : Tester la communication au sein d'un réseau

La commande ping de Linux est un utilitaire simple utilisé pour vérifier si un réseau est disponible et si un hôte est joignable. Avec cette commande, vous pouvez tester si un serveur est opérationnel. Elle permet également de résoudre divers problèmes de connectivité.

14. La syntaxe de base de ping comprend ping suivi d'un nom d'hôte, d'un nom de site web ou de l'adresse IP exacte. ping [option] [hostname] or [IP address] Essayer de faire un ping google.com . Appuyez sur Ctrl + C sur votre clavier pour arrêter le processus. Consultez l'annexe sur cette partie avant de continuer
15. Vérifiez que vous avez une connexion réseau en effectuant un ping sur le localhost. Il y a 3 manières : la plus rapide est ping 0. Testez et trouvez les 2 autres manières en ligne de commande.
16. Pour demander une adresse IPv6 ou IPv4, ajoutez -6 ou -4 après la commande ping et avant un nom d'hôte/IP. Essayer avec un site web connu et notez votre remarque.
17. Consultez la commande ping -help pour voir la liste des options de la commande ping disponibles.
18. Donner et tester la commande pour modifier l'intervalle de temps entre les paquets Ping
19. Déduisez après avoir tester la commande pour Modifier la taille des paquets Ping
20. Vous pouvez utiliser le ping flood pour tester les performances de votre réseau en cas de forte charge. Trouver à l'aide du manuel, la commande pour inonder un réseau en utilisant ping pour tester les performances.
21. Déduisez à l'aide du ping -help, la commande pour arrêter automatiquement après l'envoi d'un certain nombre de paquets.
22. Trouvez de la même manière, la commande pour arrêter automatiquement après un temps spécifique

Partie 4 : Analyse et exploration d'un réseau

Nmap est un outil utilisé pour l'exploration des réseaux et l'audit de sécurité. Cet outil est généralement utilisé par les hackers et les passionnés de cybersécurité et même par les administrateurs réseau et système pour faire de l'audit. Nous étudierons ultérieurement quelques usages plus avancés en cours de Cybersécurité. ☺

Faites apt install nmap pour procéder à son installation.

23. Sans options, Nmap révèle les services et les ports ouverts sur le ou les hôtes donnés. Essayez nmap larmand.fr et comparez à nmap google.fr
24. Consultez la commande nmap -h pour voir la liste des options de l'outil nmap disponibles.
25. Trouver dans le guide, la commande pour trouver des informations sur le système d'exploitation
26. Trouver dans le guide, la commande pour scanner une plage d'adresse au lieu d'une seule adresse IP
27. Faites la déduction de la commande qui permet d'analyser un sous-réseau entier en une seule fois.
28. Que fait cette commande ? nmap 192.168.0.* --excludefile /monFichier.txt
29. Trouver dans le guide, la commande pour détecter les paramètres du pare-feu
30. Trouver dans le guide, la commande pour trouver des informations sur les versions de service
31. Trouver dans le guide, la commande pour identifier les noms d'hôtes
32. Trouver dans le guide, la commande pour trouver une liste d'interfaces et de routes pertinentes.
33. La commande ci-après nmap -oG /home/euphraim/Bureau/ResultatScan larmand.fr permet d'enregistrer les résultats d'un scan dans un fichier sur le Bureau d'une VM Linux. Adapter la commande pour enregistrer un scan avec le flag -F du site larmand dans le fichier ResultatScanLarmand sur votre Bureau.

Partie 5 : Mise en application

A l'aide des connaissances que vous venez d'acquérir, analysez le réseau local.

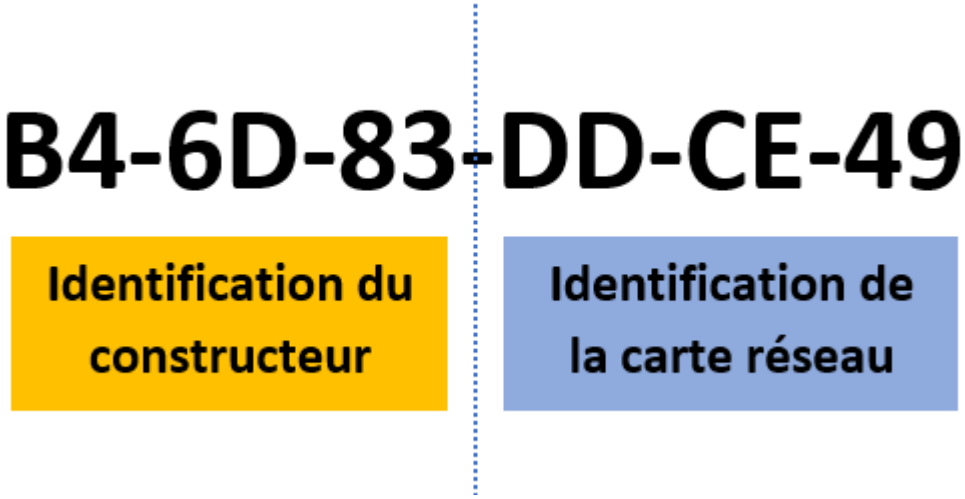
34. À l'invite de commande du terminal, saisissez la commande nécessaire pour déterminer l'adresse IP et le masque de sous-réseau de votre machine. Quel est l'adresse du réseau auquel appartient votre machine virtuelle ?
35. Saisissez la commande pour localiser les autres hôtes sur ce réseau local. Combien d'hôtes sont actifs ?
36. Répertoriez les adresses IP des hôtes qui se trouvent sur le même réseau local que votre machine virtuelle.
37. Quel est l'adresse du routeur ?
38. Répertoriez les adresses IP des imprimantes présentes sur le réseau.
39. Adaptez la commande du scan du réseau pour enregistrer les résultats dans le fichier ResultsScanSIO sur votre bureau.
40. Quelle est la commande pour enregistrer les résultats dans une base de données ?

ANNEXE DE LA MISSION 6

Informations sur les adresses MAC

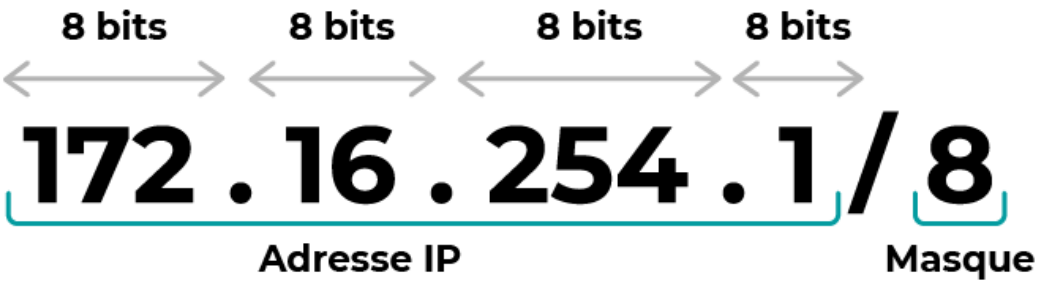
Une adresse MAC est composée de 2 parties :

- La première moitié (les 3 premiers octets) identifie le fabricant de la carte réseau.
- La deuxième moitié identifie la carte réseau elle-même.
- Je trouve le constructeur sur https://dnschecker.org/mac-lookup.php



Informations sur les adresses IP, adresse de Réseau, Masque et de diffusion

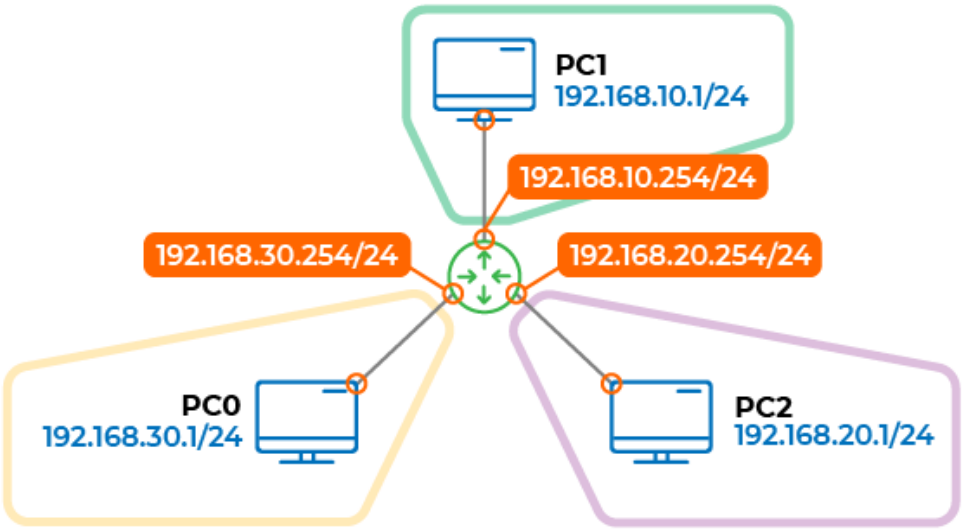
- Une adresse IP contient toujours : une partie qui identifie le réseau et une partie qui identifie la machine.
- Le masque est le délimiteur entre la partie réseau et la partie machine. C'est ce qui vous permet de vérifier que deux machines sont bien dans la même plage réseau.
- Le masque nous permet d'en déduire l'adresse réseau. Cette adresse réseau s'obtient en prenant l'adresse IP et en remplaçant par des "0" les bits identifiant la machine.



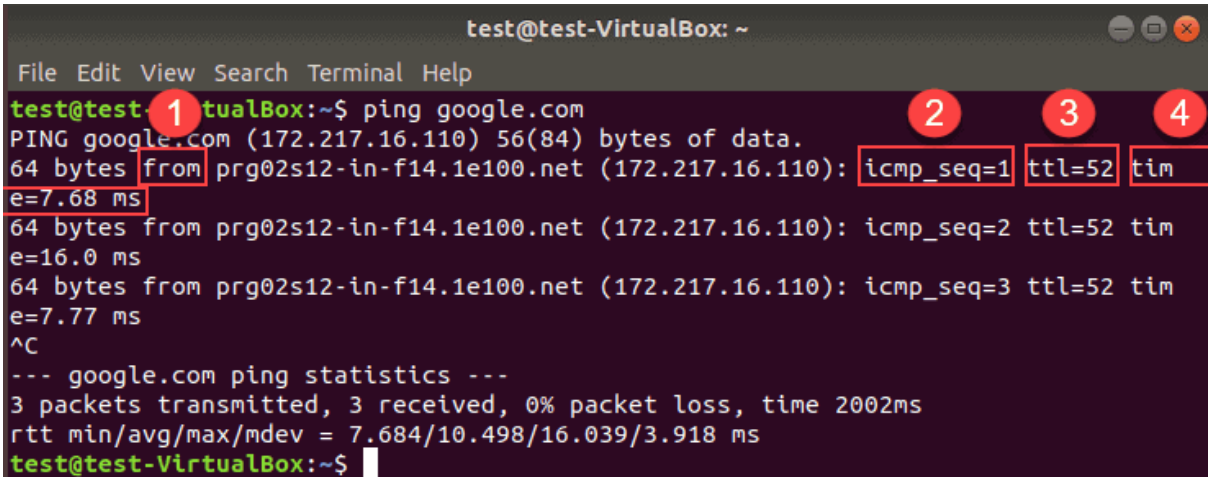
- Dans une plage réseau, la première est l'adresse du réseau et la dernière est l'adresse de diffusion.
- L'adresse de diffusion ou de *broadcast*, en anglais, sert à envoyer un message à toutes les machines d'un réseau en même temps.

Informations sur les interfaces et l'adresse de la passerelle (routeur)

- Quand on parle d'interface, on fait référence à un port physique. Exemple : le port RJ45. C'est le dispositif qui permet la communication entre deux éléments d'un système informatique. Chaque port physique ou interface doit être configuré avec une adresse IP dans le bon réseau.
- Lorsqu'un paquet est envoyé d'un réseau IP vers un autre, il passe obligatoirement par un routeur. Ce dernier est la "passerelle par défaut".



Information sur l'outil ping



from : La destination et son adresse IP. Notez que l'adresse IP peut être différente pour un site Web en fonction de votre emplacement géographique.
icmp_seq=1 : Le numéro de séquence de chaque paquet ICMP. Augmente de un pour chaque demande d'écho suivante.
ttl=52 : La valeur du Time to Live de 1 à 255. Elle représente le nombre de sauts de réseau qu'un paquet peut effectuer avant qu'un routeur ne le rejette.
time=7.68 ms : Le temps qu'il a fallu à un paquet pour atteindre la destination et revenir à la source. Exprimé en millisecondes.